

Gendarmerie

La qualité et le lien entre la gendarmerie et les élus en général, les maires en particulier, sont primordiaux pour garantir à nos concitoyens la tranquilité et la sécurité publique qu'ils sont en droit d'attendre (...). C'est dans cet esprit que le directeur général de la gendarmerie nationale a initié un certain nombre de mesures visant à formaliser les contacts".

Le groupement de gendarmerie départementale de la Haute-Garonne utilise 3 principaux réseaux sociaux afin de promouvoir des bonnes pratiques en matière de sûreté ainsi que les dispositifs mis en oeuvre au profit de la population : Opération Tranquilité Vacances, Opération Séniors, etc...

Enfin, la brigade numérique de la gendarmerie est disponible pour répondre à chacun, 24h/24, 7 jours sur 7 et 365 jours par an.

Un module de messagerie instantanée est disponible sur le site internet : http://gendarmerie.interieur.gouv.fr

BRIGADE numérique Gendarmerie

QUELQUES CONSEILS DE PREVENTION



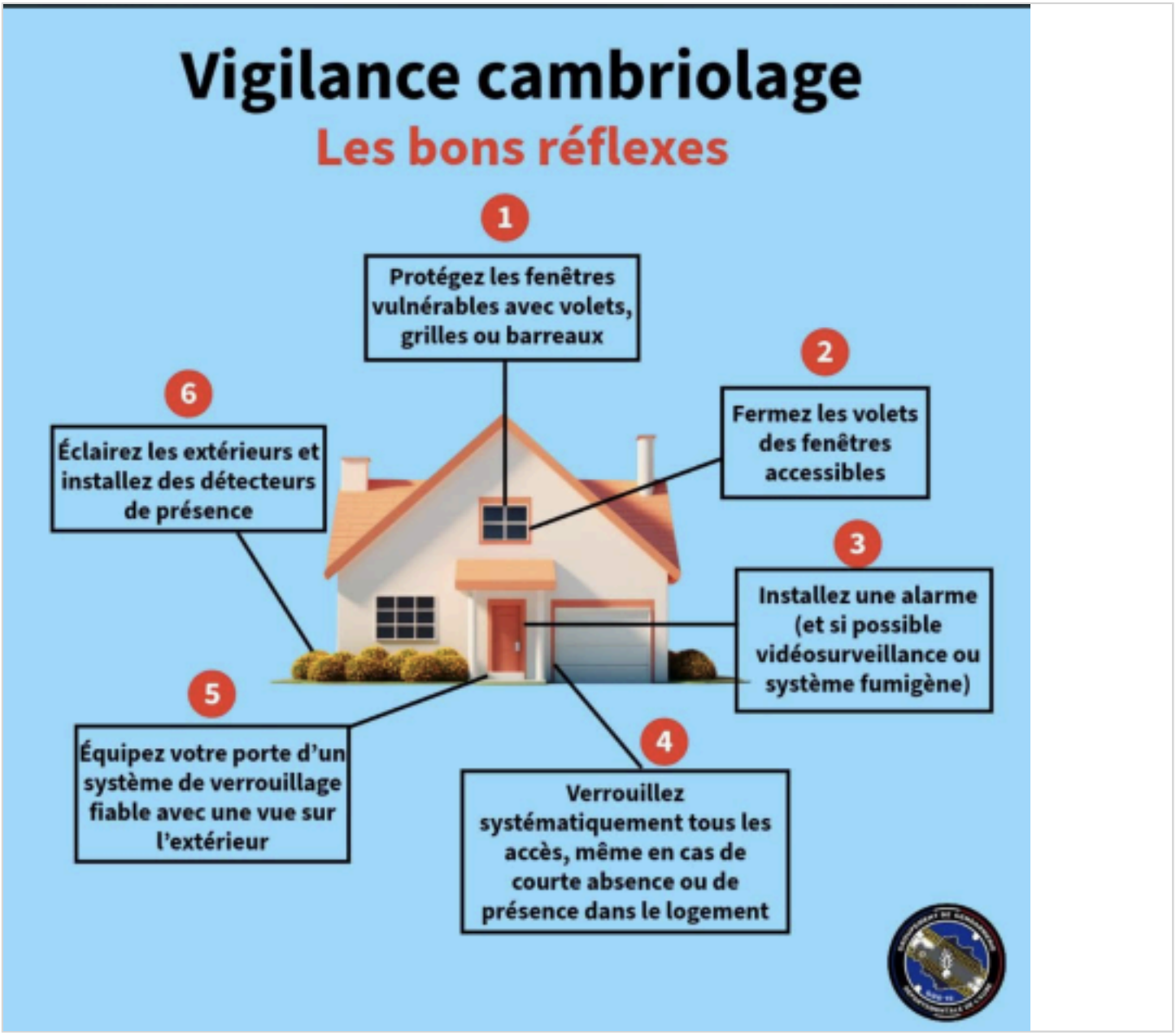
1/LES DEMARCHAGES





2/LES CAMBRIOLAGES





3/ L'UTILISATION DE LA TROTINETTE



SÉCURITÉ ROUTIÈRE VIVRE, ENSEMBLE

ÉQUIPEMENTS À TROTTINETTE ÉLECTRIQUE

OBLIGATOIRES

RECOMMANDÉS

Vêtement réfléchissant **obligatoire** la nuit ou si la visibilité est réduite, **recommandé** le reste du temps

Casque

1 PERSONNE

14 ANS MINIMUM

CASQUE AUDIO INTERDIT

TROTTOIRS INTERDITS

VITESSE DU VÉHICULE LIMITÉE À 25 KM/H
(PAR CONSTRUCTION OU PAR BRIDAGE)

Avertisseur sonore

Système de freinage

Feux de position avant et arrière

Catadioptres arrière et latéraux



LES ÉQUIPEMENTS OBLIGATOIRES EN EDPM

Les utilisateurs d'EDP non motorisés

Ils sont assimilés à des piétons. Ils peuvent circuler sur les trottoirs et sur les autres espaces autorisés aux piétons à condition de circuler à la vitesse du pas.


roller


skateboard


trottinette

Les utilisateurs d'EDP motorisés

à partir de 14 ans


overboard


monoroue


gyropodes


draisienne


trottinette électrique

Les équipements



CODES ROUSSEAU



4/LA CYBERSECURITE



MINISTÈRE
DE L'INTÉRIEUR

ALERTECYBERGEND 80
Groupement de gendarmerie départementale de la Somme

CYBERATTAQUES DOPÉES PAR INTELLIGENCE ARTIFICIELLE

LE DANGER S'INTENSIFIE, ÊTES-VOUS PRÊT ?



L'intelligence artificielle a profondément transformé le paysage des menaces. Hameçonnage ultra-réaliste sans aucune faute, usurpations vocales et visuelles (deepfakes), ou encore exploitation automatisée des failles de sécurité : les **attaques** sont désormais industrialisées, plus rapides et accessibles **à moindre coût**.

Particuliers comme **professionnels** sont ciblés.

6 RÉFLEXES ESSENTIELS POUR VOUS PROTÉGER

1 - Mettez à jour sans attendre :	MAJ	Installez systématiquement les correctifs logiciels pour fermer la porte aux failles exploitées par l'IA.
2 - Verrouillez vos accès :	LOGIN ×4	Utilisez des mots de passe robustes et uniques, gérés via un coffre-fort, et activez la double authentification (2FA).
3 - Ne confiez aucune donnée personnelle à un chatbot :		Ne confiez jamais d'informations personnelles, médicales ou professionnelles sensibles à une IA publique.
4 - Paramétrez la confidentialité de l'assistant d'IA :		Désactivez l'historique et refusez l'utilisation de vos données pour l'entraînement des modèles.
5 - Limitez ce que les applis d'IA peuvent toucher :		Limitez les autorisations d'accès des outils d'IA à vos fichiers et téléchargez-les uniquement sur les stores officiels.
6 - Vérifiez par un canal tiers :		Face à une demande d'argent urgente (même portée par une voix connue), prenez la peine de le rappeler pour authentifier son identité par un canal sécurisé.

ADOPTER LES BONS RÉFLEXES, C'EST GARANTIR SA CYBERSÉCURITÉ !





FUITE DE DONNÉES PERSONNELLES

Vos informations valent de l'or... Protégez-les !

Une fuite de données personnelles, c'est la divulgation ou le vol d'informations vous concernant : nom, adresse, numéro de téléphone, e-mail, données bancaires, etc.

Ces données peuvent être utilisées pour vous arnaquer, vous usurper ou vous cibler avec des publicités ou des fraudes.

LES BONS RÉFLEXES

Ensemble, réduisons les risques !

1 Restez vigilants face aux SMS ou e-mails suspects



Méfiez-vous des messages qui créent l'urgence, qui semblent inhabituels ou qui proviennent d'expéditeurs inconnus.

2 Ne cliquez jamais sur des liens suspects



Même si le message semble authentique, ne cliquez pas sur les liens. Ils peuvent installer des malwares ou vous rediriger vers des sites frauduleux.

3 N'ouvrez pas les pièces jointes de mails suspects



Les pièces jointes peuvent contenir des virus ou des logiciels malveillants capables de voler vos données.

4 Ne donnez aucune information par téléphone



Aucune entreprise sérieuse ne vous demandera vos identifiants, vos coordonnées bancaires ou vos mots de passe par téléphone.

5 En cas de doute, effectuez un contre-appel



Si vous recevez un appel ou un message suspect, raccrochez et appelez vous-même l'organisme concerné via un numéro officiel (pas celui fourni dans le message).

6 N'effectuez aucune manipulation sur vos comptes à la demande d'une personne par téléphone



On ne vous demandera jamais de valider un code, de modifier vos paramètres ou de faire un virement par téléphone. C'est presque toujours une arnaque.

AUTRES CONSEILS UTILES

Utilisez des mots de passe solides
Et différents pour chaque compte. Pensez aussi à l'authentification à deux facteurs.

Protégez vos appareils
Mettez à jour vos systèmes et vos applications, et utilisez un antivirus.

Limitez le partage de vos données
Sur les réseaux sociaux et les sites internet. Pensez à vos paramètres de confidentialité.

Surveillez vos comptes
Vérifiez régulièrement vos relevés bancaires et vos activités en ligne.

Parlez-en autour de vous
La vigilance est l'affaire de tous. Plus on en parle, moins on est piégé !

Vos données personnelles sont précieuses. Protégez-les, c'est protéger votre sécurité !



MINISTÈRE DE L'INTÉRIEUR

FUITES DE DONNÉES : LES BONS RÉFLEXES SI JE SUIS VICTIME

RÉAGIR VITE, LIMITER LA FRAUDE

1 SÉCURISER MES COMPTES

- Changer le mot de passe du service concerné ;
- Si réutilisé ailleurs : changer aussi ;
- Activer la double authentification (MFA), pour vos comptes, messagerie, applications.

2 DÉJOUER LES ARNAQUES « POST-FUITE »

- Méfiance : SMS/mail/ appel "urgent", provenant de "banque", "assurance", "mutuelle", etc.
- Ne jamais donner le code (SMS / mot de passe / numéro de CB / données sensibles) à des personnes qui vous contactent inopinément ;
- Recontacter via le site, l'application ou le numéro de téléphone officiel. Ne jamais utiliser le lien proposé.

3 SURVEILLER CE QUI COMPTE

- Activer les alertes (banque, achats en ligne) ;
- Vérifier les opérations / connexions inhabituelles ;
- En cas de doute : prévenir sa banque.

4 ÊTRE GUIDÉ, SIGNALER

- Si fraude/usurpation : conserver les preuves (captures écran, messages, etc.), déposer plainte (police/gendarmerie) et trouver de l'assistance sur 17Cyber.gouv.fr (24/7) ;
- Réflexe : 17Cyber, Ma Sécurité, appel 17 ;
- Si vos données apparaissent sur des plateformes en ligne, demander leur suppression au site / service qui diffuse vos informations ;
- Ressources : CNIL et Cybermalveillance.gouv.fr.

Ma Sécurité
Application Grand Public
(24/7)

17 CYBER
(24/7)

COMCYBER-MI